ICNL

www.icnl.org
info@icnl.org

COMMENT

Lesotho's Computer Crime and Cybersecurity Bill, 2021

Introduction

Lesotho's Parliament is currently considering adoption of the Computer Crime and Cybersecurity Bill, 2021. The Bill was published for a brief public comment period in late August. The stated purpose of the Bill is to combat computer crime and ensure cybersecurity by 1) establishing the National Cybersecurity Advisory Council and National Cyber Security Incident Response Team, 2) designating and protecting critical information infrastructure, 3) providing a comprehensive list of offenses committed through the misuse of electronic devices, 4) prescribing procedural standards relating to search and seizure of data, and 5) limiting the criminal liability of service providers for cybercrimes.

This comment is not a comprehensive analysis. Rather, the analysis will highlight provisions that pose a particular risk for civil society and civic space, and compare them with international legal standards, especially those governing the rights to the rights to freedom of expression and privacy.

Key concerns in the Bill are:

- The criminalization of false information, which gives the government broad discretion to censor speech;
- Other overly vague offenses, such as the expansive definition of "cyberterrorism" and broad prohibition of "racist and xenophobic" material, which provide the government with broad discretion to determine that an individual has committed an offense; and
- Conditions for exemption from intermediary liability, such as requiring a hosting provider to report to the relevant authority all illegal information on its platform,

which may prompt internet intermediaries to surveil and censor their users, thus undermining the rights to privacy and freedom of expression.

International Law

Article 19 of the International Covenant on Civil and Political Rights (ICCPR) enshrines the right to freedom of expression, which encompasses the right to hold opinions without interference, and the freedom to seek, receive, and impart information and ideas of all kinds through any medium regardless of frontiers.[1]

States are obligated to guarantee the right to freedom of expression. The Human Rights Committee has stated that "any restrictions on the operation of websites, blogs, or any other internet-based electronic or other such information dissemination systems" must comply with Article 19.[2]

Restrictions on the speech and expressions guaranteed in Article 19 are lawful only when such restrictions pass a three-part, cumulative test derived from Article 19, as follows:

> (1) **Principle of legality:** the restriction must be clearly articulated in the law such that a person reading the law can easily understand how to comply with the law and the consequences of violating the law;
>
> (2) **Principle of legitimacy**: the restriction must pursue one of the purposes set out in Article 19(3) of the ICCPR, namely: (i) to protect the rights or reputations of others; or (ii) to protect national security or public order, or public health or morals; and
>
> (3) **Principle of proportionality**: the restriction must be proven as the least restrictive means required to achieve the purported aim.[3]

The UN Human Rights Committee has stated that the burden lies with the State to show that any law or regulation restricting the freedom of expression passes Article 19's three-part test.[4]

Article 17 of the ICCPR protects the right to privacy. The protection of the right to privacy is essential to the full realization of the right to freedom of expression; undue interference with individuals' privacy can have a chilling effect on their willingness to develop, exchange, and access ideas.[5] Any limitations on the right to privacy must also pass the three-part test noted above, where the legitimate purposes for restricting the right to privacy are (i) to protect national security, public order, public health or morals, and the rights and freedoms of others.[6]

---

[1] Nigeria acceded to the ICCPR in 1993.
[2] Human Rights Committee, *General Comment No. 34: Article 19: Freedoms of opinion and expression*, UN Doc . CCPR/C/GC/34 (2011), para. 43.
[3] See, e.g., United Nations Human Rights Council, *Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, U.N. Doc. A/HRC/17/27 (2011), para. 69.
[4] General Comment No. 34, supra note 2, at para. 27.
[5] See United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the freedom of opinion and expression, Frank La Rue*, A/HRC/23/40 (2013), Part A ("Interrelations between the rights to privacy to freedom of opinion and expression")
[6] See *id.* at Part B ("Permissible limitations to privacy and freedom of expression").

Analysis

CRIMINALIZATION OF FALSE INFORMATION

ISSUE: Section 43 on the publication of false information is vaguely drafted and grants the government broad discretion to determine that information or data is "false." The criminalization of publishing false information is also a disproportionate means to further a legitimate goal, such as protecting the rights and reputations of others.[7]

ANALYSIS: International experts on the freedom of expression have definitively stated that criminalizing the dissemination of false information is incompatible with international standards for restrictions on the freedom of expression and should be abolished.[8] Laws that restrict "false" content, like this Bill, could restrict the freedom of expression by stifling independent media, especially those outlets and reports that are critical of government policies; creating a chilling effect on public debate; and undermining government and public accountability where critical views are deemed false or misleading to the public, among other effects. This is because false content laws often provide the government with broad discretion to determine whether information is false.

Section 43 of the Bill is not a permissible restriction on the freedom of expression under international law. The provision fails the principle of legality because the terms "false, deceptive, misleading, or inaccurate" are not clearly defined, making it difficult for a person reading the law to understand how to comply with the provision. This ambiguity grants the Government broad discretion to determine that a person has published "false" information and committed an offense under the Bill. For example, the Government could categorize political satire as "false" or "inaccurate" information that has the intent to mislead the public, even though political satire purposefully uses humor, irony, exaggeration, or ridicule to analyze contemporary politics. Section 43 also fails the principles of legitimacy and proportionality because criminalizing false, deceptive, misleading, or inaccurate information is not the least restrictive means to achieve a legitimate aim such as protecting the rights and reputations of others. For example, an alternative and less restrictive way to protect the rights and reputations of others would be to use civil defamation law rather than criminal measures to curb false information such as defamation; civil defamation law could provide for penalties such as apologies, corrections, and damages to the person injured by the publication of false information.

RECOMMENDATION: Remove Section 43.

---

[7] Section 43 states "A person who publishes information or data presented in a picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with intent to threaten, abuse, insult, mislead or deceive the public, or conceals commission of such an offence, commits an offence and is liable, on conviction, to a fine not exceeding M500,000 or imprisonment for a term not exceeding five years or both."

[8] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda*, FOM.GAL/3/17 (2017), para. 2(a).

OTHER OVERLY VAGUE OFFENSES

CYBERTERRORISM

ISSUE: Section 27 on cyberterrorism is vaguely drafted, granting the government broad discretion to determine whether an individual has committed cyberterrorism. The provision is also a disproportionate means to protect national security because it could prohibit legitimate forms of expression. [9]

ANALYSIS: The United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism recommends that ""terrorist offences" should be confined to instances where the following three conditions cumulatively meet: (a) acts committed with the intention of causing death or serious bodily injury, or the taking of hostages; (b) for the purpose of provoking a state of terror, intimidating a population, or compelling a Government or international organization to do or abstain from doing any act; and (c) constituting offences within the scope of and as defined in the international conventions and protocols relating to terrorism. Similarly, any criminalization of conduct in support of terrorist offences should be restricted to conduct in support of offences having all these characteristics."[10]

Section 27 fails the proportionality test of Article 19 because it adopts a broader definition for cyberterrorism than the one recommended by the Special Rapporteur by criminalizing the mere communication of information that could "destabilize or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization." This definition of cyberterrorism is much broader than acts that are intended to cause death or serious bodily harm and is, therefore, disproportionate to the aims of safeguarding national security or punishing political violence. Rather, Section 27 unduly restricts the freedom of expression because it could prohibit the communication of information, such as an editorial article that criticizes Lesotho's constitutional monarchy, labeling legitimate speech as cyberterrorism. Modeling the definition of cyberterrorism on the Special Rapporteur's recommendation would be a less restrictive means of protecting national security. For example, "cyberterrorism" could refer to "the use of a computer and information system to (a) communicate information with the intention of causing death or serious bodily injury, or the taking of hostages; (b) for the purpose of provoking a state of terror, intimidating a population, or compelling a Government or international organization to do or abstain from doing any act." This more limited definition of cyberterrorism would help ensure that the Government is empowered to combat cyberterrorism while respecting and protecting legitimate forms of expression.

Section 27 also fails the principle of legality under the three-part test for permissible restrictions on the freedom of expression because its terms are overly vague, making it difficult for a person to understand how to comply with the provision. For example, the

[9] Section 27 states "Any person who willfully and without lawful excuse uses a computer and information system to communicate information intended to seriously intimidate a population, destabilize or destroy the fundamental political, constitutional, economic or social structures of a country or an international organization or cause attacks upon persons which may lead to death, intimidation or kidnapping commits an offence and is liable, on conviction, to imprisonment for a term not exceeding twenty years."

[10] United Nations Commission on Human Rights, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, E/CN.4/2006/98 (2005), para. 72.

phrase "destabilize or destroy the fundamental political, constitutional, economic or social structures" under Section 27 could encompass a wide range of speech, such as criticism of Lesotho's current ruling political party, the All Basotho Convention, because it might "destabilize" existing "political and constitutional structures," Lesotho's close economic ties with South Africa because it could harm the country's "economic structures," or gender inequality because it could destroy "social structures." These terms are so vague that the government can arbitrarily apply Section 27 to prohibit communication of any information that it finds disagreeable.

RECOMMENDATION: Revise this provision to more precisely define cyberterrorism. Consider adopting the definition recommended by the Special Rapporteur as suggested above.

RACIST AND XENOPHOBIC MATERIAL

ISSUE: Section 35 and 36 broadly criminalize actions that may be racist and xenophobic, which overly restricts the freedom of expression.[11]

ANALYSIS: Article 20(2) of the ICCPR prohibits the advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility or violence. The Committee on the Elimination of Racial Discrimination has emphasized that the "criminalization of forms of racial expression should be reserved for serious cases, to be proven beyond a reasonable doubt."[12] States should use the following six factors to determine the severity necessary to criminalize serious hate speech: the social and political context at the time of speech, the speaker's standing in the context of the addressed audience, the speaker's intention, the degree to which the speech was provocative and direct and the form, style, and nature of arguments deployed, the extent or reach of the speech, and the likelihood of imminent harm directly stemming from the speech.[13] Moreover, any measures addressing hate speech must still respect international legal requirements for permissible restrictions on the freedom of expression.[14]

---

[11] Section 35 states "a person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification –

(a) Produces racist or xenophobic material for the purpose of its distribution through a computer system ;
(b) Offers or makes available racist or xenophobic material through a computer system;
(c) Distributes or transmits racist or xenophobic material through a computer system;
(d) Distributes racist or xenophobic material that may constitute a threat through a computer system;

Commits an offence and is liable on conviction, to imprisonment for a term not exceeding ten years or a fine not exceeding M5,000,000 or both.

Section 36 states "A person who intentionally and without lawful excuse publicly, through a computer system, uses language that incites attacks and insults to-

(a) Persons for the reason that they belong to a group distinguished by race, color, descent, national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or
(b) A group of persons which is distinguish [sic] by any of these characteristics,

Commits an offence and is liable, on convition, to imprisonment for a term not exceeding ten years or a fine not exceeding M5,00,000 or both.

[12] Committee on the Elimination of Racial Discrimination, *General Recommendation No. 35*, CERD/C/GC/35 (2013), para. 12.

[13] See United Nations General Assembly, *Promotion and protection of the right to freedom of opinion and expression: Note by the Secretary General*, A/74/486 (2019), para 14 (citing the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence,

[14] General Recommendation No. 35, supra note 14, para. 20.

Offenses under Section 35 may not meet the severity necessary for criminalization because the provision effectively bans all types of racist and xenophobic speech, regardless of the context in which the speech is conveyed. Without consideration of context, such as through the six factors noted above, the provision could prohibit the legitimate exercise of the freedom of expression, such as posting racist or xenophobic material for educational purposes or even posting xenophobic comments without the intention to incite violence against the subject of the comments.[15] This provision fails the principle of proportionality because banning all types of racist and xenophobic speech and thus banning some forms of legitimate speech is not the least restrictive means to prohibit hate speech. Rather, the provision should prohibit racist and xenophobic speech where the severity is based on an analysis of the six factors noted above. Such an approach would place fewer restrictions on the freedom of expression while supporting Lesotho's obligation under Article 20(2) of the ICCPR to prohibit hate speech.

Section 36 criminalizes language that may incite "insults" based on several characteristics. Although the ICCPR requires the prohibition of "insults" where that expression "clearly amounts to incitement to hatred or discrimination,"[16] Section 36 merely criminalizes "insults" and is therefore an overbroad application of the concept of hate speech—Article 19 of the ICCPR protects "deeply offensive" or insulting speech.[17] Similar to Section 35, the prohibition of all "insults" based on a person's characteristics fails the principle of proportionality because it is not the least restrictive means to address hate speech. Since "language that incites attacks" under Section 36 could already include insults that incite attacks, there is no need to include "insults" separately under Section 36, especially as the freedom of expression protects insulting speech.

RECOMMENDATION: Revise Section 35 to include an intent element. Remove the incitement of insults as an offense under Section 36.

LIABILITY OF SERVICE PROVIDERS

ISSUE: Part VII of the Bill protects service providers from liability for cybercrimes committed by their users but places some conditions on the service providers, which may prompt them to surveil and censor their users, thus restricting the freedoms of privacy and expression.[18]

ANALYSIS: Service providers, such as internet and telecommunications service providers, facilitate individual access to search engines, social networks, and other communications resources. Holding service providers liable for offenses committed using their services by third parties (otherwise known as intermediary liability) essentially mandates service providers to proactively surveil and censor their users—this infringes on the right to privacy

[15] United Nations Human Rights Committee, *General Comment No. 34: Article 19: Freedoms of opinion and expression*, CCPT/C/GC/32 (2011), para. 11 (clarifying that "deeply offensive" speech is still protected under Article 19 within the boundaries of Article 20(2) on hate speech).
[16] Promotion and protection of the right to freedom of opinion and expression, A/74/486, supra note 8, at para. 17.
[17] *General Comment No. 34*, supra note 9, at para. 11.
[18] Section 69(1)(b) exempts a hosting provider from criminal liability for information stored at the request of a user if the hosting provider expeditiously informs the authorities of illegal information stored on its services upon obtaining knowledge or awareness of the information.

and freedom of expression of users of communications services. To protect the freedom of expression and other rights while balancing the legitimate need of governments to address digital crimes, civil society groups drafted the Manila Principles on Intermediary Liability, which lay out safeguards and best practices for treatment of intermediary liability while protecting human rights. Principle 1 of the Manila Principles states that intermediaries should be shielded from liability for third-party content.

Although Part VII of the Bill generally exempts service providers from liability for cybercrimes committed by their users in accordance with the Manila Principles, the section places some problematic conditions on the exemption. For example, Section 69(1) places a condition on hosting providers to report any illegal information on their platforms, which may encourage hosting providers to broadly surveil and censor their users' websites because they fear that they will be held liable for any illegal content that the service provider did not "catch" and report. This restriction on privacy rights and expression fails the principle of proportionality because requiring service providers to surveil and censor their users is not the least restrictive means to achieve a legitimate aim. A less restrictive measure would be to simplify Part VII to generally provide for intermediary liability for third party content where the intermediary has not been involved in modifying that content, as recommended under the Manila Principles, Principle 1(b).

RECOMMENDATION: Remove Sections 69(1)(b). Revise Part VII to generally provide for intermediary liability for third party content where the intermediary has not been involved in modifying that content.

OTHER ISSUES:

- The Offenses under Section 21 (illegal access) and Section 22 (illegally "remaining" on a computer system) do not make a clear exception for whistleblowing or other legitimate government oversight activities by journalists and other civil society members.
- Section 38 (unsolicited messages) seems to be aimed at reducing spam and scams by criminalizing the use of a computer system to relay or transmit multiple electronic messages with the intent to deceive or mislead or use an electronic device that does not reflect the origin of such messages. However, the provision also exempts businesses from committing this offense if the act is "done within customer or business relationships." This exception should be removed, as the provision would seem to allow business to send messages with the intent to deceive and there does not appear to be a legitimate reason for this allowance.
- Articles 59 to 66 under Part VI provide some guidance on law enforcement's power to search and seize computer systems, devices, or data. However, only Article 66 provides detailed limitations and requirements for obtaining a warrant; other provisions reference other laws such as the Penal Code and the Constitution. These articles and all other relevant laws should be reviewed to ensure that they include procedural safeguards for search and seizure prescribed under international law, namely the requirement to obtain a court-issued warrant based on a reasonable suspicion of an infraction of the law before search and seizure, with details on the

material that will be surveilled directly related to the crime being investigated, limits on the duration of the warrant, and requirements to destroy the material seized following the conclusion of the investigation.

- Section 70(e) exempts a caching provider from criminal liability for the automatic, intermediate, and temporary storage of information if the provider expeditiously removes or disables access to information it has stored upon obtaining knowledge that the information at the initial source of the transmission has been removed from the network or access to the information has been disabled. This exemption should be modified to require the caching provider to remove the information only if the provider has "actual knowledge" that the information has been removed or disabled at the initial source.[19] Requiring "actual knowledge" will help balance the caching provider's mission to provide internet users with quick access to information through storing high demand information with their obligation to remove content that may infringe on fundamental human rights or undermine legitimate public concerns.

Conclusion

ICNL is grateful for the opportunity to comment on this Bill and stands ready to provide further guidance as necessary.

[19] See, e.g., Directive 2000/31/EC of the European Parliament and of the Council (8 June 2000), Article 13(1)(e).